PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-171909**

(43)Date of publication of application : **26.06.1998**

(51)Int.Cl. **G06F 19/00**

G06F 15/00

G06F 17/60

G09C 1/00

H04L 9/32

(21)Application number : **09-271437**

(22)Date of filing : **03.10.1997**

(71)Applicant : **SAMSUNG ELECTRON CO LTD**

(72)Inventor : **YU JU-YEOL**
CHUNG HO-SUK
MOON SOON-IL

(30)Priority

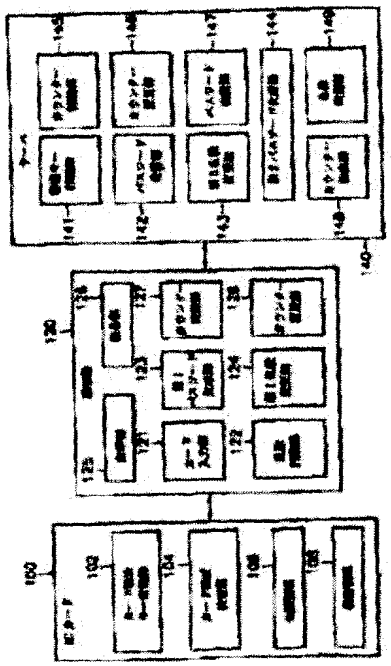
Priority number : **96 9644125** Priority date : **05.10.1996** Priority country : **KR**

(54) USER AUCENTICATION DEVICE AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To perform safe user aucentication at a low cost by providing a password receiving part for receiving a once password generate from a terminal, and a password verification part for verifying whether the received password and a generated password are identical, or the like.

SOLUTION: This device is composed of an IC card 100 for portable device for safely storing personal secret information, the easily-portable terminal 120 having a complex function capable of referencing to remains of electronic money not only generating the once password for confirming the status of an individual, and a server 140 for verifying the once password generated by this terminal 120 and providing an application service. Then, the password receive part 142 receives the once password displayed on the display part 125 of the terminal 120 via a telephone line or the like. The password verifying part 147 inspects the once password by comparing the received password and the generated password whether or not to be identical.



[Claim(s)]
[Claim 1]An IC card which has stored a secret key and a predetermined random number for generating a password for 1 times, Terminal equipment which generates a password for 1 times by considering this IC card as an input, Are a server which attests a password for 1 times generated from this terminal equipment an included user authentication device, and said terminal equipment, A card input part which performs an interface which receives said IC card and from which said IC card distinguishes whether it is the card inputted first, A random number stores dept. which reads and stores a random number of said IC card when said IC card is first inserted in said card input part, and deletes a random number of said IC card, The 1st password generation part which reads a random number stored in a secret key and said random number stores dept. of said IC card, and generates a password for 1 times by a predetermined method, The 1st random number changing part which is made to change into a predetermined value a random number value stored in said random number stores dept., and is made to store in said random number stores dept. when a password for 1 times is generated from said 1st password generation part, A secret-key stores dept. which possesses at least an indicator which displays a processing result of said terminal equipment and a server, and stores a secret key by which said server was first stored in said IC card, the same secret key as a predetermined random number, and a random number, The 2nd password generation part which reads a secret key and a random number which were stored in said secret-key stores dept., and generates a password for 1 times by same method as a predetermined method in said terminal equipment, The 2nd random number changing part which will change a random number value identically to a random number changing part of said terminal equipment, and will store a random number value of said secret-key stores dept. in said secret-key stores dept. if a password for 1 times is generated from said 2nd password generation part, A password receive section which receives a password for 1 times generated from said terminal equipment through a telephone wire or a predetermined network, A user authentication device providing a password verification part which verifies whether said received password and said generated password are the same at least, and attesting whether a user is a just user.
[Claim 2]The user authentication device according to claim 1 which said IC cards are a warrant card and electronic money combination, and is characterized by having stored safely a secret value for a user's social position attestation.
[Claim 3]The user authentication device according to claim 1, wherein a purveyor of service inserts a secret key of said terminal equipment in said terminal equipment in a user registration process.
[Claim 4]A card approach key stores dept. which possesses a secret field which requires a card approach key in order for said IC card to allow approach of a public area and the exterior which can approach unconditionally, and stores safely a card approach key required for approach of said secret field, A card approach inspection section which compares a card approach key inputted from said outside with a card approach key stored in said card approach key stores dept., and opts for permission or denial of approach of inside information is provided further, A random number stores dept. of said terminal equipment will read and store a random number and a card approach key of said IC card, if said IC card is first inserted in said card input part, The user authentication device according to claim 1 being a random number stores dept. which deletes a random number stored in a public area of said IC card, and a card approach key.
[Claim 5]The user authentication device according to claim 1, wherein said terminal equipment

possesses further a reference part which refers for the balance and the dealings items of said IC card.
[Claim 6]The user authentication device comprising according to claim 1 or 4:
A symmetrical key cryptopart which the 1st password generation part of said terminal equipment reads a secret key of said IC card, and a random number of said random number stores dept., and generates a code for said secret key and a random number using a symmetrical key cryptographic algorithm.
A hash function part which transforms a code generated from said symmetrical key cryptopart by a one-way hash function, and prevents inverse tracking of said secret key.
A code outputted from said hash function part including a format conversion part changed into a predetermined format that it is easy to read a user the 2nd password generation part of said server, A symmetrical key cryptopart which reads a secret key and a random number which were stored in said secret-key stores dept., and generates a code for said secret key and a random number using a symmetrical key cryptographic algorithm.
A format conversion part which changes into a predetermined format a code outputted in a code generated from said symmetrical key cryptopart from a hash function execution part which prevents inverse tracking by a one-way hash function, and said hash function execution part.

[Claim 7]A counter stores dept. which stores a counter value for said terminal equipment and a server to double a synchronization of terminal equipment and a server, A counter changing part which is made to change said counter value into a predetermined value whenever it generates a password for 1 times once, and is made to store in said counter stores dept. is provided further, A format conversion part of said 1st password generation part and a format conversion part of the 2nd password generation part, Provide further a counter insert portion which inserts a counter value of said counter stores dept. in a password bit string outputted from said hash function execution part, and said server, A counter extraction part which extracts a counter value from a password for 1 times received by said password receive section, When a counter value extracted from said counter extraction part and a counter value of said server are not in agreement, The user authentication device according to claim 6 providing further a random number synchronizer which generates a random number which ****s in said extracted counter value, and is made to input into a symmetrical key cryptopart of said server.
[Claim 8]The user authentication device according to claim 6 or 7, wherein said format conversion part changes the number of binary numbers into a decimal number.
[Claim 9]Said terminal equipment and a counter insert portion of a server, Carry out additional insertion of the PTS bit which shows a protocol of a password generation algorithm for at least 1 1 time or more, and a counter extraction part of said server, The user authentication device according to claim 7 which extracts said PTS bit further and is characterized by said terminal equipment and the 1st and 2nd password generation part of a server being password generation parts which generate a password for 1 times by a password generation algorithm for 1 times according to information on said PTS.
[Claim 10]An IC card which stores a secret key characterized by comprising the following for generating a password for 1 times, and has a predetermined random number, A user authentication method in a user authentication device containing a server which attests a password for 1 times which had stored terminal equipment which generates a password for 1 times by considering said IC card as an input, and same secret key and a random number as said IC card, and was generated from said terminal equipment.
A stage which inserts said IC card in said terminal equipment.
It is an input judgment stage at the beginning which judges whether said IC card was first inputted into said terminal equipment.

A password generation phase which generates a password for 1 times after performing predetermined service initialization at first in an input judgment stage at said beginning at the time of an input, and generates a password for 1 times when it is not an input at first.
A stage of receiving a password for 1 times generated from said terminal equipment through predetermined communication media, and verifying a password for said 1 times.

[Claim 11]When said IC card possesses further a card approach key required for approach to a secret field, service initialization of said password generation phase, A stage which reads a card approach key for approaching a random number and a secret field from a public area of said IC card, and is stored in terminal equipment, From a stage of deleting a random number stored in a public area of said IC card, and a card approach key of said public area, become and IC card secret-key read-out of said password generation phase, A stage of making a card approach key stored in said terminal equipment inputting into said IC card, A card approach inspection stage of allowing card approach if a card approach key inputted into said IC card and a card approach key of said IC card secret field are the same, The user authentication method according to claim 10 consisting of a stage which will read said IC card secret key if approach is permitted in said card approach inspection stage.
[Claim 12]When a counter for said terminal equipment and a server to double a synchronization of terminal equipment and a server is provided further, the 4th step of password generation for 1 time of said password generation phase, Change said random number and a counter value into a predetermined value, are a stage stored in terminal equipment and the 5th step of password generation for 1 time of said password generation phase, A stage which inserts said counter value in said password bit string outputted from the 3rd step, From a stage changed into a predetermined format, become a password value in which said counter value was inserted, and a receiving step of said verification stage, An extraction step which extracts a counter value from a received password for 1 times, A stage which compares with a counter value of said server a counter value extracted from said extraction step, When a counter value is not in agreement in said comparison step, a counter value of said counter is made the same, Provide further a stage of changing said random number value into a random number value which ****s in said counter value, and a value change stage of said verification stage, A stage which inserts said counter value in a password bit string which is a value change stage which changes said random number into a predetermined value, and is stored in terminal equipment, and is outputted by a conversion stage of said verification stage performing said one-way hash function, The user authentication method according to claim 10 or 11 consisting of a stage of changing into a predetermined format a password value in which said counter value was inserted.

JP-A-10-171909

(54) [TITLE OF THE INVENTION] USER AUTHENTICATION APPARATUS AND METHOD THEREOF

(57) [ABSTRACT]

[PROBLEM] The present invention provides a user authentication apparatus in which an IC card and a mobile terminal having an electronic money balance and trade inquiry function and a first-time password generating function are used and a method thereof.

[SOLVING MEANS] A user authentication apparatus according to the invention includes an IC card 100 in which a secret key and the like are stored, a terminal 120, and a server 140. The terminal 120 includes a card input unit 121 that receives the IC card, a random number storage unit 122 that reads a random number and stores the random number therein, a first password producing unit 123 that produces a first-time password, a first random number changing unit 124 that changes the random number value, and a display unit 125 that displays a processing result. The server 140 includes a secret key storage unit 141 in which a secret key and the like are stored, a second password producing unit 144 that produces a first-time password, a second random number changing unit 143 in which the random number value is stored, a password receiving unit 142 that receives the first-time password, and a password verifying unit 147 that verifies the password.

100 IC CARD

102 CARD PROXIMITY STORAGE UNIT

104 CARD PROXIMITY CHECKING UNIT

106 PUBLIC REGION

108 SECRET REGION

120 TERMINAL

125 DISPLAY UNIT

121 CARD INPUT UNIT

122 RANDOM NUMBER STORAGE UNIT

123 FIRST PASSWORD PRODUCING UNIT

124 FIRST RANDOM NUMBER CHANGING UNIT

126 INQUIRY UNIT

127 COUNTER STORAGE UNIT

128 COUNTER CHANGING UNIT

140 SERVER

141 SECRET KEY STORAGE UNIT

142 PASSWORD RECEIVING UNIT

143 SECOND RANDOM NUMBER CHANGING UNIT

144 SECOND PASSWORD PRODUCING UNIT

148 COUNTER EXTRACTING UNIT

145 COUNTER STORAGE UNIT

146 COUNTER CHANGING UNIT

147 PASSWORD VERIFYING UNIT

149 RANDOM NUMBER SYNCHRONIZING UNIT

[0001]

[TECHNICAL FIELD TO WHICH THE INVENTION PERTAINS] The present invention relates to a user authentication system, particularly to a user authentication apparatus in which an Integrated Circuit (IC) card and a mobile terminal having an electronic money balance and trade inquiry function and a first-time password generating function are used and a method thereof.

[0002]

[PRIOR ART] With the advances of computer and communication and widespread of a computer network, various application fields are generated by development of a technique of an Integrated Circuit (hereinafter referred to as IC) card having a memory and a computing function, and various kinds of convenience are provided to people. A function of inquiring a balance of an electronic purse and trade contents is required for electronic money that is of a kind of application field of the IC card.

[0003] A user can manage money in a user's account without going directly to a bank, and the user can easily perform many desired jobs of the user at home by long-distance connection using a computer. At this point, it is necessary for a service provider (such as a bank and a network server) to confirm whether the user who wants service is an authorized user. When attack of a person disguised as the authorized user is successfully performed due to poor performance of the user authentication system,

not only invasion of privacy but also spiritual and physical serious damage of a person are generated. Particularly, when the user wants the service from a distance, a method for clearly confirming user authentication without directly meeting the user is required for the service provider.

[0004] What only the user knows, what only the user has, or a physical feature or a habit of only the user is utilized in order to authenticate the user. Conventionally, the utilization of a password is a basic, general method used to authenticate the user. In the password method, the user is authenticated by confirming the password that is known only by the user. That is, the user who wants the service initially selects the password that is known only by the user and registers the password in the service provider (server). Usually the user uses a number or a character of several digits as the password. The user who wants to conduct the authentication transmits the password remembered by the user to the server, and the server authenticates the user by comparing the transmitted password to the user's password registered at the beginning of the service.

[0005] A first-time password in which the password is changed every time the user conducts the authentication is used in order to safely conduct the user authentication. Because the password is changed every time the user conducts the authentication, even if the attacker knows the

password once, the attacker cannot use again the password next time. In order to conduct the user authentication using the first-time password, it is necessary for the user to have a device that can produce the first-time password. At this point, when the user uses each user's first-time password producing terminal, what only the user knows and what only the user has are simultaneously confirmed in order to conduct the user authentication. Therefore, a security level can considerably be enhanced.

[0006] Unlike the existing password, a variable that is changed every time is required in order to produce a different password in the first-time password. For this reason, there are a method in which a time (RTC, Real Time Clock) is used and a method in which a random number is used.

[0007] The time the terminal possessed by the user and the server of the service provider are matched with each other is used in the user authentication method in which the time is used as the variable. That is, the first-time password is generated by the time in the terminal at the time the user conducts the authentication, and the server simultaneously generates the password, thereby comparing the first-time password and the password to conduct the user authentication.

[0008] A random number value that is produced with a random number generator in order to generate the first-time password is used in the method in which the random number

is used. When the user authentication is started, the server produces the random number value to transmit the random number value to the user. The terminal produces the first-time password by encrypting the random number value using a secret value shared with the server, and the terminal transmits the first-time password to the server. The server generates a password using the secret value shared with the terminal and the random number value transmitted by the server, and the server compares the password to the password generated by the terminal, thereby conducting the user authentication.

[0009]

[PROBLEM TO BE SOLVED BY THE INVENTION] However, there are many problems in the currently widespread user authentication method in which the password is used. Because usually the number or character of several digits, for example, personal information (such as telephone number, a date of birth, and a resident registration number) is used as the password, the third party easily analogizes the password. The user records the password somewhere so as not to forget the password selected by the user, the third party knows the password through the recorded password. When the user transmits the password from a distance through a telephone line or a computer network in order to conduct the user authentication, the password is easily known through wiretapping.

[0010] In the user authentication method in which the time

(RTC, Reel Time Clock) is used, it is necessary that the time of the terminal possessed by the user and the time of the server of the service provider be correctly matched with each other for the purpose of the first-time password generation and the user authentication. When the terminal possessed by the user and the server of the service provider are not synchronized even if the time elapses, because the first-time password produced from the terminal is not matched with the password produced from the server, the user authentication fails even for the authorized user. Thus, a particular device is required to synchronize the terminal and the server. Accordingly, in the existing application service, a special server is required to match the times of the terminal and server in order to strengthen the user authentication using the first-time password, which becomes a large economic burden on the service provider. Additionally, in the terminal that produces the first-time password using the time, because the variable is the time, the first-time password can be used only in the first-time password generator that is used for only one application service in one terminal. When the user wants various kinds of application service, disadvantageously the terminal is required in each kind of the application service.